EOSDIS Element Name

INFORMATION TECHNOLOGY SECURITY

CONTINGENCY PLAN

(TEMPLATE)

Organization Title and Code

Month, Year

Administratively Controlled Information

This document contains sensitive information and shall be handled in a way that precludes its disclosure to the general public and limits its circulation. NASA entities must attach the NASA Form 1686, Administratively Controlled Information (ACI) form to the cover of this document.

EOSDIS Element Name

INFORMATION TECHNOLOGY (IT)
SECURITY CONTINGENCY PLAN
(TEMPLATE)

Organization Title and Code

Prepared by:

____

(Name) Date
(Title)
(Organization)

Reviewed by:

____

(Name) Date
(Title)
(Organization)

Approved by:

____

(Name) Date
(Title)
(Organization)

This page intentionally left blank

Preface

Proposed changes to this document shall be submitted to the ESDIS Computer Security Official (CSO) along with supporting materials justifying the proposed revision. These changes will be issued by Documentation Change Notice (DCN), or where applicable, by complete revision.

Questions concerning this document and proposed changes shall be addressed to:

Clayton Sigman
ESDIS IT Security Official
NASA GSFC Code 423
Greenbelt, MD 20771

(301) 614-5309
Clayton.Sigman@gsfc.nasa.gov

Change Information Page

Issue	Date	Pages Affected	Description
Original			

This page intentionally left blank

List of Affected Pages

Page No.	Revision	Page No.	Revision	Page No.	Revision	Page No.	Revision

This page intentionally left blank.

Table of Contents

Section 1. Introduction

Section 2. Assumptions

Section 3. Recovery Teams

Section 4. Staffing

Section 5. Vendor Services

Section 6. Location of Off-site Vital Records

Section 7. Restoration Procedures

Section 8. Inventory

Section 9. Movement of Vital Records

Section 10. Contracts

Section 11. Equipment

Section 12. Connectivity

Section 13. Test Procedures

Section 14. Contingency Plan Modification

Section 15. Distribution

Appendix A: Recovery Team Responsibilities/Checklists

Appendix B: Contact List

Section 1. Introduction

This template is meant to be used by ESDIS Elements as a guide for preparing a Contingency Plan. Some sections require no more than inserting information into the appropriate text, while others require more detailed explanation relevant to the element's organization.

1.1 Scope

This document is the Information Technology (IT) Security Contingency Plan for (element name) located at (address). It has been developed in compliance with the NASA Procedures and Guidelines, Security of Information Technology (NPG 2810.1) and OMB Circular A-130, Appendix III, and covers all critical business functions performed by (element name) for the EOSDIS project as identified in (contract agreement or memorandum of understanding identification).

This plan establishes the procedures and identifies personnel necessary to respond to an unexpected and undesirable emergency or disaster that could prevent the (title of organization) ITS and networks from providing the expected level of service. This plan is applicable to the following (title of organization) facilities.

Facility	Building & Room

1.2 Use of the Plan

The plan covers the following types of unplanned and undesirable events:

- Total and partial loss of system hardware, software and data.
- Total and partial loss of office space.
- Non-availability of office space and/or system hardware, software and data.
- Non-availability of employees.

The types of threats covered by this plan include:

- Natural disasters such as hurricanes, tornadoes, snow storm, floods, or earthquake.
- Disruption of necessary utility services such as electric power, water, telephone, sewer, heating, and cooling.
- Disruption to normal operations such as employee sabotage, unauthorized access to system resources, and computer viruses.
- Theft of system hardware, software or data.

This plan does not cover contingencies for any classified processing. For information on such contingencies contact the responsible Directorate Secure Program Manager (SPM).

This plan is not intended to address minor events that are routinely handled by the on-duty personnel.

1.3 Restoration

This plan is specifically designed to guide personnel through a recovery effort of EOSDIS business functions. At the onset of an emergency condition, employees and resources will be able to respond quickly to any condition which could impact the ability to perform critical functions. The procedures contained herein have been designed to provide clear, concise and essential directions to recover from varying degrees of interruptions and disasters, and have the following objectives:

- To ensure the life/safety of all employees throughout the emergency condition, disaster declaration, and recovery process.
- To reestablish the essential business related services provided by (title of organization) within their required recovery window as identified in the recovery section at the declaration of disaster.
- To suspend all non-essential activities until normal and full business functions have been restored.
- To mitigate the impact to customers through the rapid implementation of effective recovery strategies as defined herein.
- To reduce confusion and misinformation by providing a clearly defined command and control structure.
- To consider relocation of personnel and facilities as a recovery strategy of last resort.

This plan is organized as follows:

Staffing:		
	Notification Procedures	Section 3 and Appendix B
	Relocation Site	Section 2.2
	Funding	Section 4
System Restoration:		
	Software and Applications	Section 8
	Configuration Requirements	Section 11
	Network Connectivity	Section 12
Business Process		
	Vital Records Identification	Section 9
	Vital Records (Off-site)	Section 6
	Supplies	Section 5
	Backup Site Contract(s)	Section 10

Restoration Procedures

Contingency Plan Administration:

Section 2. Assumptions

2.1 Assumptions

The contingency plan was developed under certain assumptions in order for the plan to address a broad spectrum of disaster scenarios. A disaster is defined as a disruption of normal business functions where the expected time for returning to normalcy would seriously impact the ability to maintain customer commitments and regulatory compliance. The recovery and restoration program is designed to support a recovery effort where access to normal facilities and data at the onset of the emergency condition is not available. The assumptions are:

Sample assumptions:

- Based on the premise that any resources required for the restoration of business functions will reside outside of the primary facility.

- That any vital records required for recovery can either be retrieved or recreated and moved to the recovery facility within 24 hours.

2.2 Critical Dependencies

The implementation and administration of this plan depends on the following:

- Development of a Contingency Response Management Team
- Training of personnel on the overall concept of the ITS Contingency Plan implementation, and individual responsibilities
- Creation of response teams
- Availability of salvage equipment in each building
- Availability of plastic to cover hardware, software and information resources.

2.3 Recovery Strategies

In order to facilitate a recovery regardless of the type or duration of disaster, (organization name) has implemented multiple recovery strategies. These strategies are categorized into three types. Each type is designed to provide an effective recovery solution equally matched to the duration of the emergency condition.

- **Type 1: Short-term Outage (Ride-out)** (Identify a length of time)
  A short term outage is defined as the period of time when computerized operations are not required, or where an outage window of the (length of time) or less would not allow adequate time to restore or use automated recovery operations.

- **Type 2: Medium-term Outage (Temporary)** (Identify a length of time)
  A medium-term outage is defined as the period of time that (organization name) will execute its formal disaster recovery strategy, which includes actually declaring a disaster. A disaster may either be declared company wide or only for the affected department or building. The decision to declare a disaster will be based on the amount of time/expense that is required to implement the formal recovery and the anticipated impact to business over this period of time.

- **Type 3: Long-term Outage (Relocation)** (Identify a length of time)
  A long-term outage is defined as the period of time that (organization name) will exceed the allowed occupancy time of its primary recovery strategy. During this phase of recover, a physical move of personnel and resources will be initiated.

2.4 Alternate Processing Facility

Arrangements have been made with (name of alternate processing site) located at (address) to provide support to (element name's) customers in case of outages exceeding (length of time), until (element identity) has restored business functionality.

2.5 Declaration Initiatives

The decision for implementing any of the three types of recovery strategies to support the restoration of business functions is based on the following:

- Every reasonable effort has been made to provide critical services to customers by first attempting to restore the primary facility and/or operate using short-term outage procedures.

- After all reasonable efforts have failed to restore the primary facility, and using manual procedures severely degrades client support, a recovery strategy that requires the relocation of personnel and resources to an alternate recovery facility will be invoked.

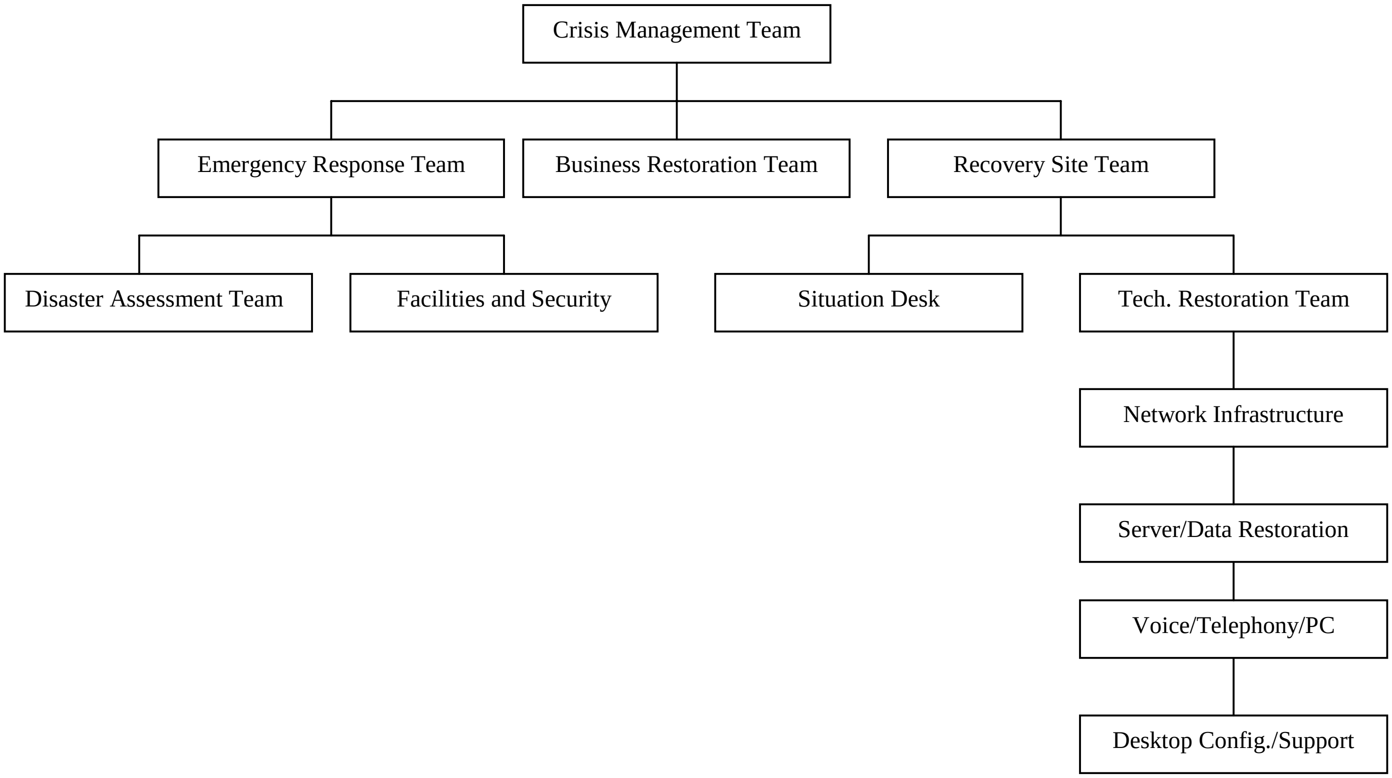
- If the outage will clearly extend past an acceptable period of time, a declaration of disaster will immediately be made.

Section 3. Recovery Teams

3.1 Recovery Team Overview

During an emergency each team member contributes the skills that they use in their everyday work to the overall response. The organization of the recovery teams is provided in the chart below:

Example:



3.2 Staff

The names of appointed leaders, each member's assigned duties, and contact information for each member is provided in Appendix (B) of this Plan. Detailed responsibilities for each team are located in Appendix (A).

Example:

A. The Crisis Management Team is organized to effectively manage and implement emergency procedures and recovery activities. The team is composed of the Contingency Response Director, Contingency Response Manager and the Team Leader of each Contingency Response Team. The Contingency Response Director is (position identification). The Contingency Response Manager is the alternate Team

Leader. The Team Leader is responsible for briefing management on the status of emergency or disaster recovery activities and providing coordination as necessary.

B. The Emergency Response Team is first on scene to assess the damage caused by the disaster or ensure precautionary measures are taken in light of any impending disaster (e.g. inclement weather, etc.) Once the ERT determines the extent of the disaster, they will either order an evacuation of the facility or work with facilities to mitigate the effects.

C. The Recovery Site Team provides support for both the physical site and technology issues. The members of this team will ensure that the alternate site is ready, and adequate for arriving recovery personnel. The RST will be the first at a meeting point or alternate site in order to register arriving personnel.

D. The Business Restoration Team consists of personnel from each area deemed critical to the continuation of critical business processes. The captains of the BRT get updated status from the Emergency Response Team to pass on to their team members to ensure prompt recovery of each area.

Section 4. Staffing

4.1 Recovery Site Staffing

Describe plans for having staff available at a backup location. Include the funding sources to cover travel, lodging, per diem, overtime, and other associated costs.

Section 5. Vendor Services

5.1 Vendor Support Services

The following is a list of vendors, suppliers, and support service contracts normally used in processing.. Arrangements have been made in advance for the delivery of equipment in the event of a disaster.

Example:

Supplies

a. The following is a sample list of supplies which are required for normal operations.

Product	Device
TK50 Tape Cartridges	TK50 Drives
Toner Cartridge	Apple Laser Writer
Paper Bond (LN03 Plus)	Digital Laser No. G705-20
Toner, Kit Laser	Digital Laser No. G705-20
Maintenance Kit (LN03)	Digital Laser No. G705-20
Toner Cartridge	Laser Jet Series II (Hewlett Packard)
Line Printer Paper	CI 600 Printer
Line Printer Paper	Printronix Printer
Line Printer Paper	LG02 Digital
Printer Ribbons	Apple Imagewriter
Printer Ribbons	CI 600 Printer
Printer Paper	Tektronix (4692) Plotter
Maint Cartridge	Tektronix (4692) Plotter
Ink (Cyan, Yellow, Magenta, Black)	Tektronix (4692) Plotter
Printer Paper	Tektronix (4696) Plotter
Maint Cartridge	Tektronix (4696) Plotter
Ink (Cyan, Yellow, Magenta, Black)	Tektronix (4696) Plotter

b. The following is a sample list of supplies available from commercial sources.

Item	Source
DEI Tape Cartridges 9786-W DC600XDT Santa Clara, Ca. 95051-851	De Voke 1500 Martin Ave, Box 58051 1-800-822-3132
Plotter Paper P/N 016-891-00 3-Color Transfer Rolls P/N 016-0906-00	Tektronix, Incorporated Computer Graphics Supplies P.O. Box 1000, M/S 63-583

Wilsonville, Or. 97070
1-800-835-6100

c. The following is a list of vendors of ADP supplies.

Wright Line (computer tape accessories)
P.O. Box 2031
Worcester, Ma. 01613

JTC Corp. (computer tape labels)
649 Rahway Ave
Union, N.J. 07083

Versatec (plotter supplies - paper & chemicals)
File #3961
P.O. Box 60000
San Francisco, Ca. 94160

3M TSR1291 (computer tape)
P.O. Box 15104
Newark, N.J. 07192

Galilee Co. (tape evaluator & cleaning supplies)
17 Deerfield Road
Mendham, N.J. 07945

Standard Register Company (printer paper)
Department 142
P.O. Box 14506
Cincinnati, Ohio 45263

Imagecraft, Inc. (printer ribbons)
1006 E. Elizabeth Ave.
Linden, N.J. 07036

Printer Ribbon for DEC LG02
Model Number YC3362

Misco
One Misco Plaza
Holmdel, N.J. 07733
1-800-976-4726

Transparency File
P/N 016-0765-05

Tek (4692) Plotter
Tektronix, Inc.
700 Professional Place
Gaithersburg, Md. 20877
1-800-TEK-6100

Section 6. Location of Off-site Vital Records

6.1 Current Off-site Facilities

Identify the location of any currently used off-site facilities that store vital records needed to get the system back into operation. List the names and contact information for the personnel who have access to these facilities and include information on how to contact them at the off-site storage location. If appropriate, provide maps that give directions to these facilities.

Name and Address of Facility:

Contact Information:

Directions/map:

Section 7. Restoration Procedures

7.1 Evaluation of Disaster

This section provides personnel with clear concise step-by-step procedures to be followed in emergency/disaster situations. For each hazard, there is a brief description of the emergency response and recovery procedures. Although these are prescribed steps, personnel should use their good judgment in assessing an emergency situation and, above all, protect their personal health and safety.

Sample:

Hazard	Emergency Response	Backup and Recovery
Freezing Rain	Step 1: Monitor weather advisories. Step 2: Notify on-site employees. Step 3: Call local radio and TV stations to broadcast weather closing information for employees at home. Step 4: Place closing sign on all doors. Step 5: Arrange for snow and ice removal.	Step 1: If loss of power caused a temporary crash, re-boot the system. Step 2: Determine if data has been lost and what will need to be reprocessed. Step 3: Re-key lost data. Step 4: If necessary, obtain backup tapes for data restoral.
Tornadoes	Step 1: Monitor weather conditions. Step 2: Notify employees of potential of severe weather. Step 3: Power off equipment. Step 4: Shut off utilities (power and gas) Step 5: Instruct employees to assume protective posture. Step 6: Assess damage once storm passes. Step 7: Assist affected employees.	Step 1: If loss of power caused a temporary crash, re-boot the system. Step 2: Determine if data has been lost and what will need to be reprocessed. Step 3: Re-key lost data. Step 4: If necessary, obtain backup tapes for data restoral.
Floods	Step 1: Monitor flood advisories. Step 2: Determine flood potential to organization. Step 3: Determine employees at risk. Step 4: Cover resources with plastic to reduce damage. Step 5: Pre-stage emergency power generating equipment. Step 6: Assess damage.	Step 1: If loss of power caused a temporary crash, re-boot the system. Step 2: Determine if data has been lost and what will need to be reprocessed. Step 3: Re-key lost data. Step 4: If necessary, obtain backup tapes for data restoral.
Hurricanes	Step 1: Power off all equipment. Step 2: Listen to hurricane advisories. Step 3: Evacuate area if flooding is possible. Step 4: Check gas, water and electrical lines for damage. Step 5: Do not use telephones, in the even of sever lightning. Step 6: Assess damage.	Step 1: If loss of power caused a temporary crash, re-boot the system. Step 2: Determine if data has been lost and what will need to be reprocessed. Step 3: Re-key lost data. Step 4: If necessary, obtain backup tapes for data restoral.
Earthquakes	Step 1: Shut off utilities. Step 2: Evacuate building if necessary. Step 3: Account for all personnel.	Step 1: If loss of power caused a temporary crash, re-boot the system. Step 2: Determine if data has been

	Step 4: Determine impact of disruption.	lost and what will need to be reprocessed. Step 3: Re-key lost data. Step 4: If necessary, obtain backup tapes for data restoral.
Power Failures	Step 1: Wait 5-10 minutes. Step 2: Power off all Servers after soft shut down procedure. Step 3: Shut down main circuit located (place). Step 4: Use emergency phone line to make outgoing phone calls. Step 5: Call power company for assessment. Step 6: Locate sources of mobile power. Step 7: Contact electrical company. Step 8: Re-energize building. Step 9: Power on equipment.	Step 1: If a surge caused a temporary disk crash, re-boot the system Step 2: If a surge caused a major disk failure, initiate disk recovery. Step 3: Determine if data has been lost and what will need to be reprocessed. Step 4: Re-key lost data. Step 5: If necessary, obtain backup tapes for data restoral.
Hazardous Material	Step 1: Evacuate personnel on alarm as necessary. Step 2: Notify fire department. Step 3: Notify HAZMAT team.	Step 1: If loss of power caused a temporary crash, re-boot the system Step 2: Determine if data has been lost and what will need to be reprocessed. Step 3: Re-key lost data. Step 4: If necessary, obtain backup tapes for data restoral.
Fires	Step 1: Evacuate personnel on alarm, as necessary. Step 2: Notify fire department. Step 3: Attempt to suppress fire in early stages. Step 4: Shut off utilities. Step 5: Account for all personnel. Step 6: Search for missing personnel. Step 7: Assess damage.	Step 1: If loss of power caused a temporary crash, re-boot the system Step 2: Determine if data has been lost and what will need to be reprocessed. Step 3: Re-key lost data. Step 4: If necessary, obtain backup tapes for data restoral.

7.2 Off-site Restoral Strategy

Once the Emergency Response Team has determined that a declaration of disaster is required, the following sequence of events will occur:

Sample:

Steps	**Instruction**
1. Evacuate affected facility.	If the emergency requires an evacuation of employees, execute evacuation plans.
2. Go to staging area.	Follow building evacuation instructions.
3. Determine length of outage.	Review written and verbal damage assessment reports from facilities and civil authorities and then estimate the amount of time the facility will be uninhabitable.

4. Select disaster outage.	Based on the estimated duration of the outage, declare the disaster event as either a Type 1 (less than xxx hours), type 2 (x hours to 6 weeks), or Type 3 (6 weeks or longer)
5. Activate alternate facilities.	Contact alternate facilities. Confirm their availability and alert them of estimated arrival time.
6. Release personnel from the staging area.	Once the disaster level has been selected, release all personnel from the staging area to their assigned recovery location. • Non-essential personnel – Home • Recovery Site Team – Alternate Facility • End Users – Alternate Facility • Command Center Staff – Alternate Facility • Crisis Management Team – Alternate Facility
7. Recovery Site Team establish Command Center	RST personnel are the first to arrive at the alternate facility to setup and organize the command center prior to the arrival of the Crisis Management Team and support personnel.
8. Establish situation desk.	At the command center, establish a dedicated line with operator to field all incoming calls. Announce command center phone number to all recovery participants.
9. Review recovery requirements.	Determine on a department by department basis to determine who is most affected by the disaster. Group departments by recovery resource requirements, time frames, and co-location requirements.
10. Obtain technology shopping list.	Once the technology requirements of the affected department(s) are known, create a requirements list for the IT support staff.
11. Contact quick ship vendors.	Using the vendor list or local sources, order replacement technology indicated on requirements list.
12. Retrieve electronic/hardcopy vital records.	Retrieve vital records from locations as indicated in the Vital Records section. Have vital records shipped and staged at the alternate facility,.
13. Setup replacement LAN.	The priority of server restoration to support all other business functions is: • Core technology. • End-user servers.
14. Activate short-term recovery strategies.	Instruct each department to initiate their short-term recovery strategies. These will be used while the replacement LAN/WAN circuits are implemented.
15. Populate alternate facility.	Once the replacement LAN/WAN is functional, notify the Business Recovery Team that departments can now begin executing their Type 2 recovery strategies.

Section 8. Inventory

8.1 Software Inventory and Contacts

Identify all vendor software running on the system. Include the names of persons to contact for support. Identify any critical materials stored off-site that will be required for getting the system back online or for processing on a backup system elsewhere.

Sample:

Software/Version	**Contact**	**Location**
Windows NT 4.0	System Administrator	Bldg 15. Room 30
Windows 2000	System Administrator	Bldg 4. Room 166
HP-UX 2.5	System Administrator	Bldg 4. Room 166

Section 9. Movement of Vital Records

9.1 Records Identification

Identify any hardcopy documents that should be gathered and moved to the backup site to facilitate recovery and operations. (Consider keeping copies of these materials prepackaged at the backup site or at another appropriate offsite location.)

Section 10. Contracts

10.1 Contracts for Backup Site

Include copies of any contracts or agreements for any backup sites for processing, hardware or software maintenance, copies of leases, and license information. Also, include a copy of the offsite storage facility contract.

10.2 Contract Review

Contracts will be reviewed at least annually. Identify the date of the last review.

Section 11. Equipment

11.1 Packing and Moving Equipment

Include instructions on packing of any equipment which must be moved to the backup site. If qualified movers have been pre-selected, provide the agreement and notification information for the movers.

11.2 Equipment Configuration for Restoration

Include all necessary configuration information for restoring the equipment at the backup site, such as hardware, operating systems, software applications, hubs or switches, cabling, etc. If the backup site has the equipment that will be used, include a copy of the agreed upon configuration at the backup site.

Section 12. Connectivity

12.1 Connectivity Requirements

Include lists and diagrams of required connectivity.

12.2 Communications Requirements

State how voice communications will be maintained with management and customers.

Section 13. Test Procedures

13.1 Test Plan

The purpose of the Test Plan is to ensure that the Contingency Plan remains current, and that it can address each contingency covered in this plan. In order to ensure complete knowledge and ability to carry out the emergency and disaster recovery activities identified in this plan, (title of organization) will test the plan. The (specify position title) will initiate an unannounced drill that will simulate an ITS emergency or disaster. The test will assess the:

- Ability of the Contingency Response Management Team to assess an emergency situation and implement appropriate response procedures.

- Practicality of planning, assumptions, and procedures.

- Degree to which roles and responsibilities have been adequately defined.

13.2 Objective

Provide detailed procedures that allow the consistent and meticulous exercising of Contingency Plan activities under test or actual disaster conditions for each mission critical and sensitive unclassified system covered by this plan.

13.3 Scope

The scope of the testing spans all critical systems covered by the Contingency Plan, and includes procedures to test the execution and verification of the output of these efforts.

The most detailed section will be for testing of critical application systems. Specific procedures for testing will ensure the components of management, personnel, data (input, applications/systems software, output) and the equipment all remain current, accurate, and proficient for those application systems identified as critical.

13.4 Training

The (title of position) will ensure that (title of organization) personnel receive an orientation to the overall concept of the ITS Contingency Plan, its execution, and individual responsibilities. As changes to the ITS Contingency Plan are made, it is the responsibility of the (title of position) to ensure that individuals are informed.

13.5 Testing

Several levels of drills will be performed to test this contingency plan.

Level 1 Test -- Verification of all emergency phone numbers, to include: managers, members, alternates, vendors, law enforcement, fire department, back-up sites, etc.

Level 2 Test -- Determine vital personnel response time. Each team member should be required to explain their emergency reaction, response, and recovery responsibilities.

Level 3 Test -- Determine readiness of off-site storage facility and personnel.

Level 4 Test -- Run a selected critical system at the alternate/backup site.

Level 5 Test -- Simulate a major disaster and activate the emergency response procedure.

13.6 Test Frequency and Evaluation

Level 1 through 3 tests will be conducted every six months and the results/findings will be forwarded to the (title of position). Level 4 and 5 tests will be conducted annually and the results/findings forwarded to the (title of position). Element management, along with the Contingency Response Management Team, must evaluate the test results and then perform the refinements to the plan or test procedures of the team membership. It is important to quantitatively measure the test results for the amount of time required to perform various activities, accuracy of each activity, and the amount of work completed during the test period.

Section 14. Contingency Plan Modification

14.1 Contingency Plan Responsibility

The (title of position) is responsible for presenting the Information Technology Security (ITS) Contingency Plan to the management of (EOSDIS element) for review and approval.

14.2 Changes and Updates

This plan will be periodically updated, as changes in network or system configuration warrant, with time between updates not to exceed 1 year. The (title of position) is responsible for maintaining a list of changes and presenting them to the approving authorities.

14.3 Approving Authorities.

Approving authorities for changes to the (title of organization) ITS Contingency Plan are:(title of position) and (title of position).

Section 15. Distribution

15.1 Plan Sensitivity

This plan contains sensitive information and will be protected from accidental or unintended release to unauthorized individuals. The following procedures have been established to protect the plan from disclosure.

15.2 Restricted Distribution

Copies will be restricted to the following individuals or locations:

A. Element Management
B. Element Security Point of Contact
C. Systems Managers
D. Network/System Administrators
E. Center IT Security Manager (if applicable)
F. Members of the Contingency Response Management Team

15.3 Secured Storage

All copies of the plan are to be stored in locked rooms, desks, file cabinets etc, when the plan is not in use. Copies may be stored in unlocked files, desks, or similar items if they are located in a locked room.

15.4 Log of Recipients

The (title of organization) will maintain a log of ITS Contingency Plan recipients. The log will reflect the date, the copy number, and the name of the individual to whom assigned.

15.5 Return Copies Upon Release

Upon change of work assignment or termination of employment, individuals holding copies of this plan must return them to the (title or position) before being released by (title of organization).

Appendix A: Recovery Team Responsibilities/Checklists

Samples:

A1. Crisis Management Team Recovery Checklist

FUNCTION:	CRISIS MANAGEMENT
TEAM:	CRISIS MANAGEMENT TEAM
TEAM LEADER:	TBD
RESPONSIBILITIES:	The Crisis Management Team is the ultimate emergency authority. All elements report directly to the CMT and in turn, the CMT reports directly to management on the progress and status of the recovery effort. As the final decision-maker, the CMT makes decisions based upon input from the elements under its command.
RECOVERY STRATEGY:	1. Proceed to the command center and begin executing recovery procedures. 2. Officially declare a disaster emergency by contacting all teams and ordering disaster plans to commence. Plan implementation will depend upon the type and severity of disaster declared by the Manager. 3. Schedule the first CMT meeting immediately and instruct coordinators to begin implementation of their plans. 4. Remain in constant communication with management to respond to developing needs. 5. Assess the scope of the disaster and determine which recovery action should be taken, using the contingency plan. 6. Issue first daily executive status report to management to keep them apprised of the status of the disaster and the response. 7. Monitor the progress of the recovery process. 8. Assign responsibilities to the Coordinators and assess their progress in realizing their assignments. 9. Maintain a database of actions by each coordinator so that a continuing status report may be generated for the use of upper management. 10. Issue a daily “evening report” to management detailing the daily progress of the restoration efforts.
RECOVERY TECHNOLOTY:	3 phones, 1 link phone
VITAL RECORDS:	• ITS Contingency Plan • Call Lists

A2. Disaster Assessment Team Checklist

FUNCTION:	DAMAGE ASSESSMENT
TEAM:	EMERGENCY RESPONSE TEAM
TEAM LEADER:	TBD
RESPONSIBILITIES:	The Disaster Assessment Team is responsible for the accurate documentation and thorough assessment of the physical damage that would result from a disaster. Responsibilities include the Initial Disaster Assessment and the Final Disaster Assessment. The Initial Assessment is issued within a time frame established by the CMT and its focus is the speedy analysis of the disaster to assess the approximate time required to reoccupy the damaged facility. The Final Disaster Assessment is a complete report that details the cause of the disaster, remediation actions, and a detailed assessment of the damages including valuation of all damaged plant and equipment. The individual in charge must be a careful and skilled documenter who can build the Assessment Team from the diverse elements required.
RECOVERY STRATEGY:	1. Proceed to the Command Center and begin executing recovery procedures. 2. Assemble or take charge of established Disaster Assessment Team. 3. Team should consist of security personnel, photographer, videographer, area specialists (fire investigator, architect, civil engineer, etc.) and ABC Insurance Representative. 4. Verify with public security (fire and police) that your team is allowed to reenter the building. 5. Enter with a definite plan for assessment (back to front, left to right, zigzag) use a blueprint to confirm your plan. 6. Carefully document the status of the disaster taking copious notes, using portable dictating equipment, and validating findings with film and video. 7. Employ domain specialists to assist in identifying damaged equipment. 8. File completed report with the CMT.
RECOVERY TECHNOLOTY:	1 phone, 1 link phone
VITAL RECORDS:	• ITS Contingency Plan • Call Lists

A3. Technology Restoration Team Checklist

FUNCTION:	TECHNOLOGY RESTORATION TEAM
TEAM:	RECOVERY SITE TEAM
TEAM LEADER:	TBD
RESPONSIBILITIES:	The Technology Restoration Team is responsible for coordinating the recovery of the computing infrastructure. This team manages the server, networking, data, telephony, and desktop workstation recovery efforts. The team leader will work with the other restoration teams to ensure that adequate space is being acquired to recover not only personnel, but also computer and telephony equipment.
RECOVERY STRATEGY:	1. Proceed to the Command Center and begin executing recovery procedures. 2. Coordinate with Security to obtain a copy of the Damage Assessment Report. 3. Officially declare an IR disaster if appropriate. 4. Coordinate with Real Estate to determine the new location for the personnel involved and the facilities available for network hardware at the new facility (wiring closets). 5. Coordinate with the IR Domain to determine the affect on IR and the schedule for the restoration of that domain. 6. Coordinate with Insurance to assist in valuations and processes for the Damage Assessment Report. 7. Work with Domain managers to determine connectivity needs and to establish a schedule for restoration. 8. Prepare the daily IR report for inclusion in the “Daily Executive Status Report.”
RECOVERY TECHNOLOTY:	1 phone, 1 link phone
VITAL RECORDS:	• ITS Contingency Plan • Call Lists

Appendix B: Contact List

B1. EMERGENCY CHAIN OF COMMAND AND NOTIFICATION PROCEDURE

The emergency chain of command is listed below. Each individual must first determine the validity of the contingency.

The persons listed below must first determine that an emergency situation affecting the ITS exists. They have the authority to declare when that emergency situation starts and to approve the execution of the ITS Contingency Plan.

(Call in order until one is reached)

Title	Name	Office	Residence
1. Division Chief			
2. Associate Chief			
3. Branch Head			
4. Section Head			

The first person reached after having decided to start the execution of the ITS Contingency Plan would call the Contingency Response Director.

B2. Team Contact List

Upon activation of the Contingency Plan the Contingency Response Director notifies all members of Contingency Response Management Team. (see phone list below). Team Leaders notify members of their teams.

- CONTINGENCY RESPONSE DIRECTOR

Name :	Alternate :
Code :	Code :
Work Phone :	Work Phone :
Home Phone :	Home Phone :

- CONTINGENCY RESPONSE MANAGER

Name :	Alternate :
Code :	Code :
Work Phone :	Work Phone :
Home Phone :	Home Phone :

- SECURITY TEAM LEADER

Name :	Alternate :
Code :	Code :
Work Phone :	Work Phone :
Home Phone :	Home Phone :

- TECHNICAL TEAM LEADER

Name :	Alternate :
Code :	Code :
Work Phone :	Work Phone :
Home Phone :	Home Phone :

- TRANSPORTATION TEAM LEADER

Name :	Alternate :
Code :	Code :
Work Phone :	Work Phone :
Home Phone :	Home Phone :